UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/575,150	05/23/2000	Paul Lapstun	NPK004US	9212

24011 7590 12/01/2004

SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 12/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/575,150	LAPSTUN ET AL.	
	Examiner	Art Unit	
	Kyung H Shin	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 May 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7,8 and 10-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7,8 and 10-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 May 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on July 1, 2004.

2. **Claims 1- 17** are amended and **claims 6, 9** are canceled. **Claim 1** is **independent** claim.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-5 and 7, 8, 10-17** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Eldridge et al. (U.S. Patent No. 6,515,988: Filed Jul. 17, 1998) in view of Stefik (U.S. Patent No. 5,715,403: Filed Nov. 23, 1994).**

Regarding Claim 1 (Currently amended), Eldridge discloses a network connected to a printer, a first server, and a network terminal, a network terminal authorization method for authorizing the printing of a document at the printer at the request of the network terminal, including the steps of:

b) allocating, at the first server, the authorization identifier; (see Eldridge col. 5, line 65 - col. 6, line 1: authorization information exists at the server system)

d) receiving, at the first server, an authorization request from the network terminal containing the authorization identifier and the printer identifier, whereby the user of the network terminal proves physical access to the printer because the user obtained the printer identifier through physical access to the printer, thus increasing printer security; (see Eldridge col. 5, line 65 - col. 6, line 1: authorization information at the server system to process documents)

e) validating, at the first server, the authorization request; (see Eldridge col. 9, lines 53-60: verify and process a document from a first server)

f) creating, at the first server, an authorization record authorizing the network terminal to print at the printer (see col. 7, lines 1-16),

g) requesting, at the network terminal via a printing request, printing of the document at the printer; (see col. 8, lines 62-66)

h) verifying, using the authorization record, that the network terminal is authorized to print at the printer (see col. 9, lines 18-22), and that the authorization record contains the same printer identifier as the printing request; (see col. 6, lines 5-10; and col. 6, lines 48-49: *"Authorization--The general token 30 includes ... the two main security components. It provides the means by which the system can verify that the token is genuine and has not been tampered with. The first security component is an Authorizer Identifier 342-- ... indicates the person that created the token 30. ... The Authorization identifier 342 may be*

... as complex as a full X.509 identity certificate (see ITU-T Recommendation X.509--CCITT document 'The Directory-Authentication Framework'). The second security component is an Authorizer Digital Signature 344, ... a hash of the string using any suitable well-known secure hash function (e.g. MD5, SHA; see Applied Cryptography by Bruce Schneier, 1996, John Wiley and Sons), and (c) encrypt the hash with the user's private key, ")

i) in the event that the verification succeeds, allowing the document to be printed at the printer. (see col. 9, line 35; and col. 5, line 65 - col. 6, line 10: *"A token contains ... essential information which allows the system (token-capable server software resident on public networks and private networks) to initiate actions which produce the desired result. For example, printing out a document only needs a simple interaction: The document's token is selected .... When the latter token is received by the server software ..., the servers acts on the receipt of the token and causes the document to be retrieved, processed, and printed. "*
Tokens are used as security and authentication devices and control the locating and access (host location), transfer (if necessary) and processing (printing) of documents.*)*

Eldridge discloses a mechanism for accessing electronic documents within a network connected document repository for printing. (see Eldridge col. 2, lines 10-17: *" ... information necessary to access documents, to invoke a document services with appropriate parameter settings, or to initiate the actions of a*

document device .... security information which provides safeguards to ensure that unauthorized use of the documents or document services that are referenced ... ")

Eldridge does not disclose obtaining authentication information at a printer. However, Stefik discloses:

a) receiving, at the printer and at the first server, an authorization identifier request requesting the allocation of an authorization identifier; (see Stefik col. 3, lines 34-50: user site information packages (IP) containing authorization information are printed or placed onto storage media)

c) providing to a user, at the printer, the authorization identifier and the printer identifier; (see Stefik col. 3, lines 34-50)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Eldridge to obtain authorization information based on physical access to a printer or placement onto storage media as taught by Stefik. One of ordinary skill in the art would be motivated to employ Stefik in order to strengthen security in a network connected environment requiring authentication for printing access. (see Stefik col. 3, lines 35-40: " *... A plurality of encrypted information packages (IPs) ... IPs of interest are selected by the user and are decrypted and stored locally ... IPs may be printed, displayed or even copied to other storage medias ...* ")

Regarding Claim 2, Eldridge discloses a method according to claim 1, where, in the requesting step, the printing request is sent to the first server, and the verifying and sending steps are performed at the first server. (see col. 5, line 65 - col. 6, line 10: A network can contain multiple server (first server, second server,...,) with token server software installed. The token server software system controls the accessing and processing of documents based on information contained within the token and server system.)

Regarding Claim 3, Eldridge discloses a method according to claim 1, where, in the requesting step, the printing request is sent to a second server and the sending step is performed at the second server; the verifying step including the sub-steps of: see col. 9, lines 13-21)

a) requesting, at the second server and via a verification request sent to the first server, verification; (see col. 9, lines 29-37)
b) verifying, at the first server and in response to the verification request, that the network terminal is authorized to print at the printer. (see col. 9, lines 53-60: A "second" token software enabled server must receive a token to receive, verify and process a document (retrieve and/or print) from a first server that received a token to process a document.)

Regarding Claim 4, Eldridge discloses a method according to claim 1 or claim 3, including the further steps of:

a) allocating, at the network terminal, a public/private signature key pair; (see col. 2, lines 47-56)

b) storing, at the network terminal, the private signature key; (see col. 7, lines 13-15)

c) storing, at the first server and as part of the authorization record, the public signature key. (see col. 2, lines 64-67: *" The security information includes a digital signature of the information in the token. The digital signature is a digest of information in the token and its encryption with the document owner's private key. This follows well known prior cryptographic art relating to public/private key cryptography (see U.S. Pat. No. 4,405,829). "* PKI technology is used in the implementation of security and authentication for access at a network terminal.)

Regarding Claim 5, Eldridge discloses a method according to claim 4, where the requesting step includes the substep of generating a digital signature using the private key (see col. 2, lines 47-50) and attaching it to the request (see col. 7, lines 43-54), and the verification step includes the sub-step of verifying the digital signature attached to the request using the public key. (see col. 3, lines 11-19: : *" Tokens which include security information are presented to "secure documents servers". A secure server contains a "gatekeeper" which verifies signatures on tokens and examines the specified conditions ... (e.g. encrypting the document with the appropriate key). The public key for verifying the signature is obtained through a parameter in the security information which identifies the owner of the document .... "* Digital signature technology is used in the implementation of security for access file server (document retrieval and transmittal) and/or print server (document formatting and printing) system.)

Regarding Claim 7, Eldridge discloses a method according to claim 1, where the creating step includes the sub-steps of:

a) allocating a terminal identifier for the network terminal; (see col. 6, lines 48-62: *" The general token 30 includes a Service Host Identifier 32 which identifies a host machine on a network…. "* The network address (equivalent to terminal identifier) indicates the network location for the host system executing the web browser software and acting as a network terminal.)

b) storing the terminal identifier in the authorization record; (see col. 7, lines 1-16)

c) storing, at the network terminal, the terminal identifier. (see col. 1, lines 29-42; and col. 6, lines 48-49: *" The general token 30 includes a Service Host Identifier 32 which identifies a host machine on a network. "* The network address (equivalent to terminal identifier) indicates the network location for the host system executing the web browser software and acting as a network terminal.)

Regarding Claim 8, Eldridge discloses a method according to claim 7, where the authorization record is retrievable by the printer identifier and terminal identifier stored therein. (see col. 7, lines 44-54: The token contains an identifier indicating host system with attached item (document or printer).)

Regarding Claim 10, Eldridge discloses a method according to claim 9, where the creating step includes the sub-step of:

a) recording, at the first server, that the authorization identifier has been used; (see col. 7, lines 1-16)

b) the validating step includes the sub-step of rejecting, if the authorization identifier is recorded as having been used, the authorization request. (see col. 2, lines 57-60)

Regarding Claim 11, Eldridge discloses a method according to claim 9, where the step of storing the authorization identifier includes the sub-step of:

a) storing expiry information relating to the authorization identifier; (see col. 2, lines 58-60; col. 7, line 65 - col. 8, line 3)

b) the validating step includes the sub-step of rejecting the authorization request if the expiry information indicates that the authorization request id has expired. (see col. 2, lines 57-60: *" The security information can also include specified conditions that will restrict access to a document. For example, it may include (1) an expiry date beyond which access to the document is no longer granted, ... "* Expiration (time period) information is stored as an access parameter for a particular document. If the time period has expired, then access to the document is rejected during the authentication process.)

Regarding Claim 12, Eldridge discloses a method according to claim 2 or claim 3, where the requesting step includes the sub-step of including, in the printing request, the document. (see col. 9, lines 35-37: *" The document data are then sent over the network*

... , to the workstation 50 which originally received the Print Service token. "

Document data is transmitted over network to server system printing document.)

Regarding Claim 13, Eldridge discloses a method according to claim 2 or claim 3, where the requesting step includes the sub-step of including, in the printing request, a document identifier of the document. (see col. 8, lines 14-26: Document ID is included in the printing request transmitted to server system.)

Regarding Claim 14, Eldridge discloses a method according to claim 13, where the sending step includes the sub-step of retrieving the document using the document identifier. (see col. 9, lines 32-34: *" Using the Document Identifier 46, the document data (electronic file) are retrieved by the file server 52. "* Based on the document ID the actual document can be retrieved from a file server system and transmitted to a print server system.)

Regarding Claim 15, Eldridge discloses a method according to claim 14, where the sending step includes the sub-step of formatting the document for printing. (see col. 10, lines 7-18; and col. 9, lines 37-40: *" For example, printer 54 associated with transceiver 22 may be capable of printing only in PostScript.RTM. format; and step s10 therefore included adding parameters to the token designating that the data file sent ultimately to the printer must be converted to PostScript.RTM. format. Following conversion ... , the (converted) document data are sent (step s19) to the printer 54. Upon receiving the document data, the document is printed .... "* The document can require formatting before actual printing at print server system.)

Regarding Claim 16, Eldridge discloses a method according to claim 13, where the sending step consists of sending the document identifier to the printer. (see col. 9, lines 29-34: "*The document data are then sent over the network ... , to the workstation 50 which originally received the Print Service token. "* Information indicating a specific document (indicated by ID) is sent to the print server system for document printing.)

Regarding Claim 17, Eldridge discloses a method according to claim 1, where the network terminal is a Web browser running on a computer system. (see col. 4, lines 67 - col. 5, line 3; col. 5, lines 5-10: *" The invention has been implemented using conventional web browser software (e.g. Netscape) providing cross-platform communication and document transfer over the internet. However, it will be appreciated that the invention may be implemented using different system configurations: see EP'619. It ... may be a PC running Windows. ... , or a minicomputer running UNIX, ... , or any suitable processor-controlled network computer. "* A 'network terminal' is designated as a PC system or UNIX system executing a web browser software program. (e.g. Netscape or Internet Explorer) The network terminal system with token server software installed and an attached printer can print document transmitted from other systems in the network.)

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9 am - 7 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS
Kyung H Shin
Patent Examiner
Art Unit 2143

KHS
Nov. 28, 2004

Primary Examiner
Art Unit 2143
William C. Vaughn, Jr.